UPDATES ON SPAM, PHISHING AND TROJANS

M. E. Kabay, PhD, CISSP-ISSMP

In updating a chapter on spam, phishing and Trojans in a security textbook, I collected and inserted additional material that I am making available to readers here.

For 2012, Symantec reported that Android-operating-system threats (virtually unknown a decade earlier) against mobile devices increased drastically between January 2010 and the end of 2012: from fewer than 100 unique variants in about 10 families to around 4500 variants in about 170 families.[1] In addition, an increasing number of phishing scams in 2012 were being carried out through social media – a term not even mentioned in the corresponding report for the first half of 2006.[2]

* * *

A notorious spammer was Sanford "Spamford" Wallace, founder of Cyber Promotions in the 1990s, which actively used spam as a commercial service. In October 2009, Facebook won a civil suit against him for sending fraudulent messages to its users.[3] Wallace was ordered to pay $711M fine – which he was unlikely to pay because he filed for bankruptcy in June 2009.

In August 2011, he was indicted in the federal court in San Jose on

> …multiple counts of fraud and related activity in connection with electronic mail. Wallace was also charged with three counts of intentional damage to a protected computer and two counts of criminal contempt. According to the indictment, from approximately November 2008 through March 2009, Wallace executed a scheme to send spam messages to Facebook users. Those messages compromised approximately 500,000 legitimate Facebook accounts, and resulted in more than 27 million spam messages being sent through Facebook's servers. The indictment alleges that Wallace sent spam messages to Facebook users during three time periods: First, on or about Nov. 5, 2008, and continuing until approximately Nov. 6, 2008, Wallace accessed Facebook's computer network to initiate the transmission of a program that resulted in more than 125,000 spam messages being sent to Facebook users; Second, on Dec. 28, 2008, Wallace accessed Facebook's computer network to initiate the transmission of a program that resulted in nearly 300,000 spam messages being sent to Facebook users; Third, on Feb. 17, 2009, Wallace accessed Facebook's computer network to initiate the transmission of a program that resulted in more than 125,000 spam messages being sent to Facebook users.[4]

At the time of writing (May 2013), USA v. Sanford Wallace was scheduled to open on Monday June 3, 2013 in the court of Judge Edward J. Davila in the San Jose Courthouse.[5]

Symantec reported about spam as over 90% of total email traffic in 2009[6] and 2010[7], but the proportion began dropping over the next few years. In June, 2011, Symantec reported a spam rate of about 73% of total email;[8] by December 2011, they reported a further drop to about 70%.[9] According to Kaspersky Lab in early 2013, "…the share of spam in email traffic decreased steadily throughout 2012 to hit a five-year low. The average for the year stood at 72.1% - 8.2 percentage points less than in 2011. Such a prolonged and substantial decrease in spam levels is unprecedented."[10] A different study in January 2013 suggested that only about 60% of all email was spam in 2012.[11] Estimates by other experts suggested that only about 15% of the total spam was getting through all the spam filters at ISP and application levels.[12]

In "The Economics of Spam" published in the Summer 2012 issue of the *Journal of Economic Perspectives*, Justin M. Rao (Microsoft) and David H. Reiley (Google), both formerly employees of Yahoo! Research, discuss the *externality* of spam – the use of victims' resources to support profit for the criminals. They write,

> We estimate that American firms and consumers experience costs of almost $20 billion annually due to spam. Our figure is more conservative than the $50 billion figure often cited by other authors, and we also note that the figure would be much higher if it were not for private investment in anti-spam technology by firms…. On the private-benefit side, based on the work of crafty computer scientists who have infiltrated and monitored spammers' activity … we estimate that spammers and spam-advertised merchants collect gross worldwide revenues on the order of $200 million per year. Thus, the "externality ratio" of external costs to internal benefits for spam is around 100:1.[13]

* * *

The Anti-Phishing Working Group (AWPG) was founded in 2003 and is one of the most active and productive anti-phishing organizations today:

> The APWG is a worldwide coalition unifying the global response to cybercrime across industry, government and law-enforcement sectors. APWG's membership of more than 2000 institutions worldwide is as global as its outlook, with its directors, managers and research fellows advising: national governments; global governance bodies like ICANN; hemispheric and global trade groups; and multilateral treaty organizations such as the European Commission, Council of Europe's Convention on Cybercrime, United Nations Office of Drugs and Crime, Organization for Security and Cooperation in Europe and the Organization of American States. Membership is open to financial institutions, retailers, solutions providers, ISPs, telcos, defense contractors, law enforcement agencies, trade groups, treaty organizations and government agencies. APWG member benefits include: clearinghouses of cybercrime event data; cybercrime response utilities for professionals from the private, public, and NGO sectors who combat cybercrime; community-building conferences for cybercrime management professionals; public education utilities for cybercrime prevention; standards

> development for cybercrime data exchange and programs for promotion of cybercrime research.[14]

*** * ***

It was inevitable that spammers would adapt to filtering measures. By late 2012, an increasing number of spammers were distributing their spam among a large number of compromised servers, leading to the term *snowshoe spamming.* McAfee Labs summarized the problem as follows:

> Snowshoe spamming is now one of the biggest spam problems. The issue has exploded over the past two years and will continue to increase sharply due to lack of exposure by law enforcement authorities and threats of lawsuits by companies using the illegal email lists.
>
> The phenomenon is characterized by the following:
>
> - Spammers blast out millions and millions of blatantly illegal spam messages every day from newly rented hosts until they get evicted from their subnetworks or move on.
> - Recipients have their inboxes bombarded with these spam messages and are unable to opt out of them because they are not sent from a legitimate source.
> - The result of snowshoe spamming is permanently blacklisted addresses and sometimes subnetworks.
> - Because spamming is seen as simply annoying rather than malicious, authorities have largely ignored this problem, despite the growing volumes of unwanted email originating from these sources. Companies using these shady marketers have threated to file defamation lawsuits when researchers have tried to expose this activity.[15]

Criminals continue the evolution of their tools without respite; a January 2013 report found that spear phishers have applied a new tool called Bouncer that adapts their URLs to include unique identifiers for their intended victims; attempting to access the criminals' pages without a valid identifier in the URL results in a 404 (no such page) error, thus interfering with researchers' analysis of the phishing pages.[16]

In February 2013, analysts found that "When security experts looked into some of the highest profile hacks in recent years - one particular criminal group kept on coming to their attention. The Comment Group, which industry insiders say is based in China, offer hacking for hire – be it for individuals, corporations or governments…." They research individual companies or organizations to locate detailed information that allows highly specific topics and even content in the phishing messages. For example, a Coca-Cola executive reportedly opened a phishing email supposedly from his own boss; the link he clicked on downloaded spyware into his computer and allowed Chinese industrial spies to extract information which stymied the acquisition of China's largest soft-drinks company.[17]

In April 2013, the US Department of Homeland Security (DHS) warned "organizations that post a lot of business and personal information on public web pages and social media sites" not to do so. In October of 2012, phishers harvested detailed information about employees from a public posting by an energy company listing attendees at a conference. In addition to spear-phishing attacks on named individuals, "Malicious emails that appeared to be from one of the attendees were sent to others on the list informing them of a change in the sender's email address. Recipients were politely asked to click on an attached link that promptly took them to a site containing malware."[18]

The Anti Phishing Working Group (AWPG) is a valuable repository of statistical information about phishing.[19] Their report on phishing during the fourth quarter of 2013 includes the following findings (these are direct quotations formatted as bullet points with page references removed):

- Phishing attacks against online game players saw a massive increase, from 2.7 percent of all phishing attacks in Q3 to 14.7 percent in Q4.
- Financial services continued to be the most targeted industry sector in the fourth quarter of 2012 with payment services close behind.
- Online gaming credentials are valuable to certain criminals, who sell them on the black market. In-game items held in those accounts can also be sold by phishers for real-world cash. Victims can even have their real-life identities stolen.
- Attacks against social media doubled to 6%, up from 3% in the third quarter.
- During Q4, about 30 percent of personal computers worldwide were infected with malware.
- More than 57 percent of PCs in China may have been infected, while PCs in European nations were infected least often.
- Except for October 2012, the number of phishing sites declined every month from April 2012 through December 2012.
- April 2012 saw 63,253 unique phishing sites detected, falling to 45,628 in December 2012.
- The APWG received reports of 28,195 unique phishing sites in December. December's total was 31 percent lower than the high of 40,621 reports in August 2009.
- Use of crimeware dipped slightly in this quarter from the previous, as did the use of data-stealing malware.
- The use of other malware has increased by a statistically significant amount from the previous quarter.[20]

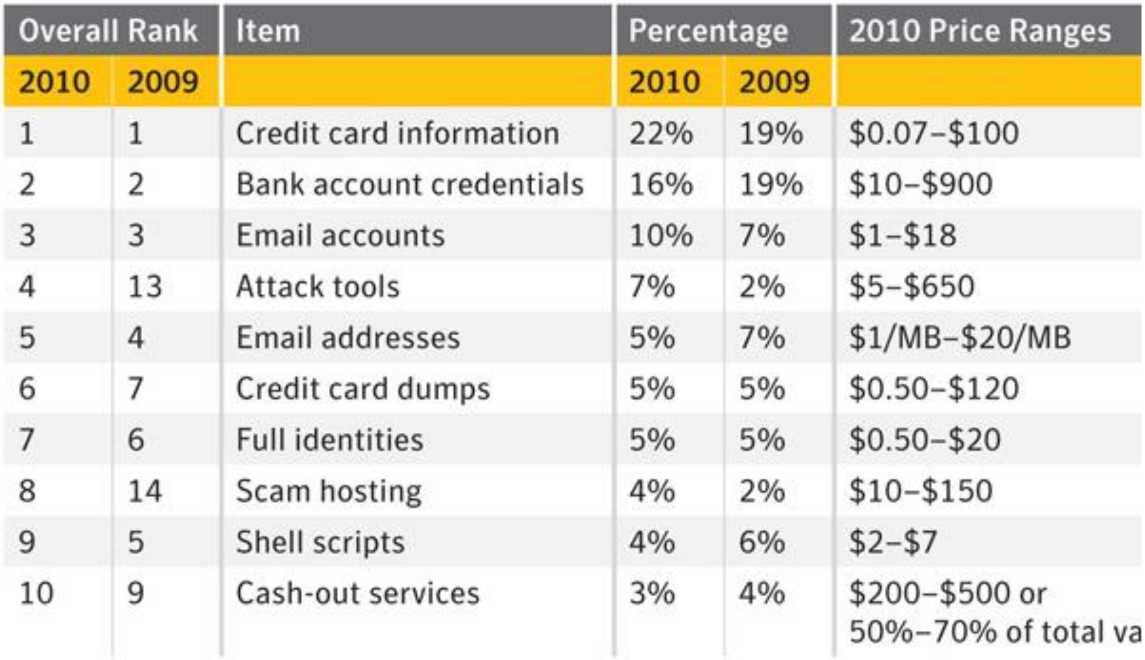
More recent reports about Trojans include the following cases and studies:

- The BackDoor.Wirenet.1 Trojan was identified in August 2012; the malware "is the first Trojan Horse program that works on the Mac OS X and Linux platforms that is ‘designed to steal passwords stored by a number of popular Internet applications.’”[21]

- The “PandaLabs Q1 Report” for 2013 found that “Trojans set a new record, causing nearly 80 percent of all computer infections worldwide. Despite their inability to replicate, Trojans are capable of triggering massive infections through compromised Web sites that exploit vulnerabilities in browser plug-ins like Java, Adobe Reader, etc. This attack method allows hackers to infect thousands of computers in just a few minutes with the same Trojan or different ones, as attackers have the ability to change the Trojan they use based on multiple parameters such as the victim’s location, the operating system used, etc.”[22]
- In March 2013, Kaspersky Labs reported that a new spyware attack on Tibetan freedom activists used a Trojan designed for the Android mobile-phone operating system.[23]
- The Flashback Trojan had infected more than 600,000 Macintosh computers by early April 2013 by exploiting a flaw in Java.[24]
- In April 2013, criminals sent out invitations to watch video footage of the Boston Marathon bombings. A remote-access Trojan was installed as a “WinPcap Packet Driver (NPF)” to evade notice.[25]
- In May 2013, Graham Cluley of Sophos reported on a Trojan (Mal/BredoZp-B) circulated in an email supposedly from Tiffany & Co. that claimed to include details of an export license and a payment invoice.[26]

Finally, there’s some interesting information on the underground economy in the following table from the Symantec "Fraud Activity Trends” published in 2010:

Table of Prices Paid for Data Traded in the Underground Economy[27]



Overall Rank		Item	Percentage		2010 Price Ranges
2010	2009		2010	2009	
1	1	Credit card information	22%	19%	$0.07–$100
2	2	Bank account credentials	16%	19%	$10–$900
3	3	Email accounts	10%	7%	$1–$18
4	13	Attack tools	7%	2%	$5–$650
5	4	Email addresses	5%	7%	$1/MB–$20/MB
6	7	Credit card dumps	5%	5%	$0.50–$120
7	6	Full identities	5%	5%	$0.50–$20
8	14	Scam hosting	4%	2%	$10–$150
9	5	Shell scripts	4%	6%	$2–$7
10	9	Cash-out services	3%	4%	$200–$500 or 50%–70% of total va

NOTES

[1] (Symantec 2013)

[2] (Turner 2006)

[3] (Associated Press 2009)

[4] (FBI 2011)

[5] (San Jose Federal Court 2013)

[6] (McMillan 2009)

[7] (Toor 2010)

[8] (Henderson 2011)

[9] (Whitney 2011)

[10] (Kaspersky Lab 2013)

[11] (Gudkova 2013)

[12] (Radicati and Hoang 2012)

[13] (Rao and Reiley 2012)

[14] (Anti-Phishing Working Group 2013)

[15] (McAfee 2012)

[16] (VERACODE 2013)

[17] (Lee 2013)

[18] (Vijayan 2013)

[19] (Anti-Phishing Working Group 2013)

[20] (Aaron 2013)

[21] (Kosner 2012)

[22] (PandaLabs 2013)

[23] (Gallagher 2013)

[24] (Silverman 2012)

[25] (Cluley, Sick malware authors exploit Boston Marathon bombing with Trojan attack 2013)

[26] (Cluley 2013)

[27] (Symantec 2010)

WORKS CITED

Aaron, Greg. "Phishing Activity Trends Report: 4th Quarter 2012." *Anti-Phishing Working Group.* 04 24, 2013. http://docs.apwg.org/reports/apwg_trends_report_Q4_2012.pdf (accessed 05 23, 2013).

Anti-Phishing Working Group. "About APWG." *APWG.* 2013. http://apwg.org/about-APWG/ (accessed 05 23, 2013).

—. "APWG Phishing Attack Trends Reports." *APWG.* 04 24, 2013. http://apwg.org/resources/apwg-reports/ (accessed 05 23, 2013).

Associated Press. "Sanford Wallace: Facebook Wins $711 Million In Case Against 'Spam King'." *Huff Post | Tech.* 10 30, 2009. http://www.huffingtonpost.com/2009/10/30/sanford-wallace-facebook-_n_339703.html (accessed 05 23, 2013).

Cluley, Graham. "Breakfast malware at Tiffany's? Trojan horses spammed out widely." *Sophos | nakedsecurity.* 05 22, 2013. http://nakedsecurity.sophos.com/2013/05/22/tiffany-malware/ (accessed 05 23, 2013).

—. "Sick malware authors exploit Boston Marathon bombing with Trojan attack." *Sophos | nakedsecurity.* 04 17, 2013.

http://nakedsecurity.sophos.com/2013/04/17/malware-boston-marathon-bombing/ (accessed 05 23, 2013).

FBI. "Sanford Wallace Indicted for Spamming Facebook Users: Self-proclaimed “Spam King” Sent More Than 27 Million Spam Messages." *FBI | San Francisco Division | US Attorney's Office | Northern District of California.* 08 04, 2011. http://www.fbi.gov/sanfrancisco/press-releases/2011/sanford-wallace-indicted-for-spamming-facebook-users (accessed 05 23, 2013).

Gallagher, Sean. "First targeted attack to use Android malware discovered: Kaspersky uncovers trojan spread by "spear-phish" to Tibet activists." *ars technica.* 03 26, 2013. http://arstechnica.com/security/2013/03/first-targeted-attack-to-use-android-malware-discovered/ (accessed 05 21, 2013).

Gudkova, Darya. "Spam in January 2013." *Securelist | Analysis.* 02 21, 2013. http://www.securelist.com/en/analysis/204792282/Spam_in_January_2013 (accessed 05 22, 2013).

Henderson, Nicole. "Symantec Report Finds Spam Accounts for 73 Percent of June Email." *Web Host Industry Review.* 06 28, 2011. http://www.thewhir.com/web-hosting-news/symantec-report-finds-spam-accounts-for-73-percent-of-june-email (accessed 05 23, 2013).

Kaspersky Lab. "Spam in 2012: Continued Decline Sees Spam Levels Hit 5-year Low." *Kaspersky Lab.* 01 13, 2013. http://www.kaspersky.com/about/news/spam/2013/Spam_in_2012_Continued_Decline_Sees_Spam_Levels_Hit_5_year_Low (accessed 05 23, 2013).

Kosner, Anthony Wing. "New Trojan Backdoor Malware Targets Mac OS X And Linux, Steals Passwords And Keystrokes." *Forbes | Tech.* 08 31, 2012. http://www.forbes.com/sites/anthonykosner/2012/08/31/new-trojan-backdoor-malware-targets-mac-os-x-and-linux-steals-passwords-and-keystrokes/ (accessed 05 23, 2013).

Lee, Dave. "The Comment Group: The hackers hunting for clues about you." *BBC | News | Business.* 02 11, 2013. http://www.bbc.co.uk/news/business-21371608 (accessed 05 23, 2013).

McAfee. "Snowshoe Spamming Emerges as Threat to Email Security." *McAfee | Business Home | Security Awareness.* 12 27, 2012. http://www.mcafee.com/us/security-awareness/articles/snowshoe-spamming-biggest-problem.aspx (accessed 05 23, 2013).

McMillan, Robert. "90 percent of e-mail is spam, Symantec says." *Computerworld | Applications.* 05 26, 2009. http://www.computerworld.com/s/article/9133526/90_percent_of_e_mail_is_spam_Symantec_says (accessed 05 23, 2013).

PandaLabs. "PandaLabs Q1 Report: Trojans Account for 80% of Malware Infections, Set New Record." *Panda Security | Press Room | News.* 05 03, 2013.

http://press.pandasecurity.com/news/pandalabs-q1-report-trojans-account-for-80-of-malware-infections-set-new-record/ (accessed 05 23, 2013).

Radicati, Sara, and Quoc Hoang. "Email Statistics Report, 2012-2016: Executive Summary." *Radicati Group.* 04 23, 2012. http://www.radicati.com/wp/wp-content/uploads/2012/08/Email-Statistics-Report-2012-2016-Executive-Summary.pdf (accessed 05 22, 2013).

Rao, Justin M., and David H. Reiley. "The Economics of Spam." *Journal of Economic Perspectives 26(3):87-100.* 2012. http://www.aeaweb.org/articles.php?hs=1&fnd=s&doi=10.1257/jep.26.3.87 (accessed 05 23, 2013).

San Jose Federal Court. "Calendar for Judge Edward J. Devila." *US Courts.* 05 23, 2013. http://www.cand.uscourts.gov/CEO/cfd.aspx?7143 (accessed 05 23, 2013).

Silverman, Dwight. "More than half a million Macs infected with Flashback Trojan malware." *Chron | TechBlog.* 04 05, 2012. http://blog.chron.com/techblog/2012/04/more-than-half-a-million-macs-infected-with-flashback-trojan-malware/ (accessed 05 23, 2013).

Symantec. "2013 Internet Security Threat Report, Volume 18." *Symantec | Security Response Publications.* 04 15, 2013. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf (accessed 05 22, 2013).

—. "Fraud Activity Trends." *Symantec | Enterprise | Security Response | Internet Security Threat Report.* 2010. http://www.symantec.com/threatreport/topic.jsp?id=fraud_activity_trends&aid=underground_economy_servers (accessed 05 23, 2013).

Toor, Amar. "Symantec Says 92-Percent of All E-mail is Spam, Phishing Attacks Declining." *SWITCHES.* 08 13, 2010. http://www.switched.com/2010/08/13/symantec-says-92-percent-of-all-e-mail-is-spam-phishing-attacks/ (accessed 05 22, 2013).

Turner, Dean. "Symantec Internet Security Threat Report, Volume X." *Symantec | White Papers.* 09 22, 2006. http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf (accessed 05 22, 2013).

VERACODE. "New Phishing Toolkit Uses Whitelisting To Keep Scams Alive." *VERACODE | the security ledger.* 01 16, 2013. https://securityledger.com/new-phishing-toolkit-uses-whitelisting-to-keep-scams-alive/ (accessed 05 23, 2013).

Vijayan, Jaikumar. "DHS warns of spear-phishing campaign against energy companies: Attackers used information from company website to craft attacks." *Computerworld | Security | Malware and Vulnerabilities.* 04 05, 2013. http://www.computerworld.com/s/article/9238190/DHS_warns_of_spear_phishing_campaign_against_energy_companies (accessed 05 23, 2013).

Whitney, Lance. "Spam sinks to lowest level in almost three years, says Symantec: The amount of spam around the globe now accounts for 70 percent of all e-mail, a sharp decline from 2009 when it accounted for 90 percent." *c|net | news | security & Privacy.* 12 07, 2011. http://news.cnet.com/8301-1009_3-57338317-83/spam-sinks-to-lowest-level-in-almost-three-years-says-symantec/ (accessed 05 23, 2013).

*** * ***

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

*** * ***